Bond Case Briefs

Municipal Finance Law Since 1971

Oklahoma Pension Fund Cyber Attack Shows Rising Risk for Munis.

- **Hackers stole $4.2M from law enforcement retirement system**
- **Cybersecurity readiness can affect credit ratings, S&P says**

Oklahoma has joined the ranks of state and local governments struck by hackers, fueling concerns about the escalating risk of such attacks on municipalities.

The Federal Bureau of Investigation is probing the cyber theft of $4.2 million from the Oklahoma Law Enforcement Retirement System, the pension fund for highway troopers, state agents, park rangers and other officers. The fund has recovered some of the money and told retirees benefits would remain intact. But the hack illustrates the state's vulnerability to bigger attacks that could carry far larger financial risks.

"Your ability to pay debt is based on trust, if the trust isn't there, it's going to be hard for everyone," said Geoffrey Buswick, an analyst for S&P Global Ratings, who has written about the risk these attacks pose for public entities. "If you have your head in the sand when it comes to cybersecurity, we're going to look at that for our rating."

The Oklahoma hack is the latest in a series of cyber breaches that show how exposed municipalities across the country are to online crime, a risk factor that rating companies are paying closer attention to as these incidents become more common. So far in 2019, municipalities have reported 73 ransomware attacks, up from 54 in 2018, according to data collected by a researcher at Recorded Future, a cybersecurity company.

Public pensions are already under stress from an uncertain investing environment and, in many cases, the growth of unfunded liabilities. State and local government retirement plans have between $1.6 trillion and $4 trillion less than what they need to cover all benefits that have been promised, depending on the interest rate used to value liabilities.

Money is constantly moving in local governments' servers to pay vendors, contractors or employees among other recurring transactions, making them a lucrative target for hackers.

In May, Baltimore residents faced disrupted services after hackers penetrated the city's systems in the second such cyberattack in less than two years. Moody's Investors Service called the incident "credit negative," citing "significant out-of-pocket expenses" expected after such a breach. Even so, Moody's didn't expect the city's financial position to be materially affected.

Greenville, North Carolina suffered a cyber attack in April, and hackers hit Atlanta in March 2018, costing the city an estimated $17 million to fix, which was about 2.6% of its budget, according to Boston-based Breckinridge Capital Advisors.

The Oklahoma pension fund, which has almost 1,500 retirees, was attacked after an employee's email account was hacked, according to the Oklahoman newspaper. Duane Michael, the fund's

executive director, told the newspaper that the money was illegally diverted.

Michael told the Oklahoman that his employees are getting training to prevent another breach. Jake Lowrey, a spokesman for the Oklahoma state agency that manages the hacked email account, declined to comment.

While the hackers took a small fraction of the Oklahoma pension's $1 billion in total assets, the theft still leaves a negative impression, according to S&P's Buswick. There's no clear-cut solution to avoid hacks, he said. Instead, it's a matter of governments identifying their weak spots, planning a reaction and determining a process for recovery.

S&P hasn't downgraded an entity based solely on cybersecurity concerns yet, Buswick said. But in April, the agency lowered its outlook to negative on Princeton Community Hospital in West Virginia after the impact of a 2017 cyberattack was reflected in its unrestricted reserves.

Moody's rates Oklahoma Aa2, or the third-highest level of investment grade, and S&P has an equivalent AA on the state. The $4.2 million loss from last month's hack isn't likely to drive a credit decision for such a large borrower, Buswick said.

Still bondholders are paying attention. While the cyber risks are hard to assess in a "meaningful" manner, they're part of investment analysis, said Matthew Stephan, the senior analyst for municipal market research at Columbia Management LLC. Protocols for these scenarios aren't always outlined for investors or written about in analysts' reports, he said.

"We kind of treat it like a low probability event -- like a 500-year weather event," he said, noting that the incidents don't typically affect the long-term price of bonds.

Other firms, like Breckinridge, include cybersecurity as part of its environmental, social and governance analysis.

"The market has become aware, investors have become aware, the media has become aware of cybersecurity issues," said Andrew Teras, a senior analyst for Breckinridge. "It's just one element of many that we're looking at but that's true of anything. We think it's very material — we consider it, and we know is a risk."

Bloomberg Cybersecurity

By Maria Elena Vizcaino

September 13, 2019, 6:36 AM PDT

Copyright © 2026 Bond Case Briefs | bondcasebriefs.com